Midterm, Math 118, Winter 2000

Robert Boltje

1. Let

$$R := \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \quad \text{and} \quad K := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}\,.$$

It is clear that R and K are commutative rings. Moreover, consider the function

$$N\colon K \to \mathbb{Q}, \quad a + b\sqrt{2} \mapsto (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2\,.$$

(a) Let $a_1, b_1, a_2, b_2 \in \mathbb{Q}$. Show that $a_1 + b_1\sqrt{2} = a_2 + b_2\sqrt{2}$ if and only if $a_1 = a_2$ and $b_1 = b_2$. (You may use that $\sqrt{2}$ is irrational)

(b) Show that K is a field.

(c) Show that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in K$.

(d) Let $\alpha \in R$. Show that $\alpha \in U(R)$ if and only if $N(\alpha) \in \{-1, 1\}$.

(e) Show that there are infinitely many units in R.

(f) Show that the function $\tilde{N}\colon R \to \mathbb{N}_0\,,\ \alpha \mapsto |N(\alpha)|$, is a euclidean norm for R.

(g) Let $\alpha \in R$. Show that if $|N(\alpha)|$ is a prime number, then α is a prime element in R.

(h) Show that each prime number $p \in \mathbb{N}$ with $p \equiv \pm 3 \mod 8$ is a prime element in R.

(i) Decompose the elements 2 and 7 of R into prime elements of R.

(j) Are there infinitely many mutually non-associated prime elements in R?

2. (a) Find a solution $a \in \mathbb{Z}$ for the congruences

$$a \equiv 9 \mod 16\,.$$
$$a \equiv 7 \mod 125\,.$$

(b) Let a be as in part (a). Compute the order of $a + 2000\mathbb{Z}$ in $U(\mathbb{Z}/2000\mathbb{Z})$.

3. (a) Find all generators of the group $U(\mathbb{Z}/7\mathbb{Z})$.

(b) Find a generator of the group $U(\mathbb{Z}/343\mathbb{Z})$. How many generators are there?